Title: Hazard Analysis

Author(s): Meredith, Austin Dean
McCallum, Jacob Bryan

Intended for: Lecture for NCS Pipeline Course at various universities.

Issued: 2018-10-15

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the Los Alamos National Security, LLC for the National Nuclear Security Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Hazard Analysis

Nuclear Criticality Safety Division

Austin Meredith

Jacob McCallum

Nuclear Criticality Safety Analysts

10/17/18

National Nuclear Security Administration

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA

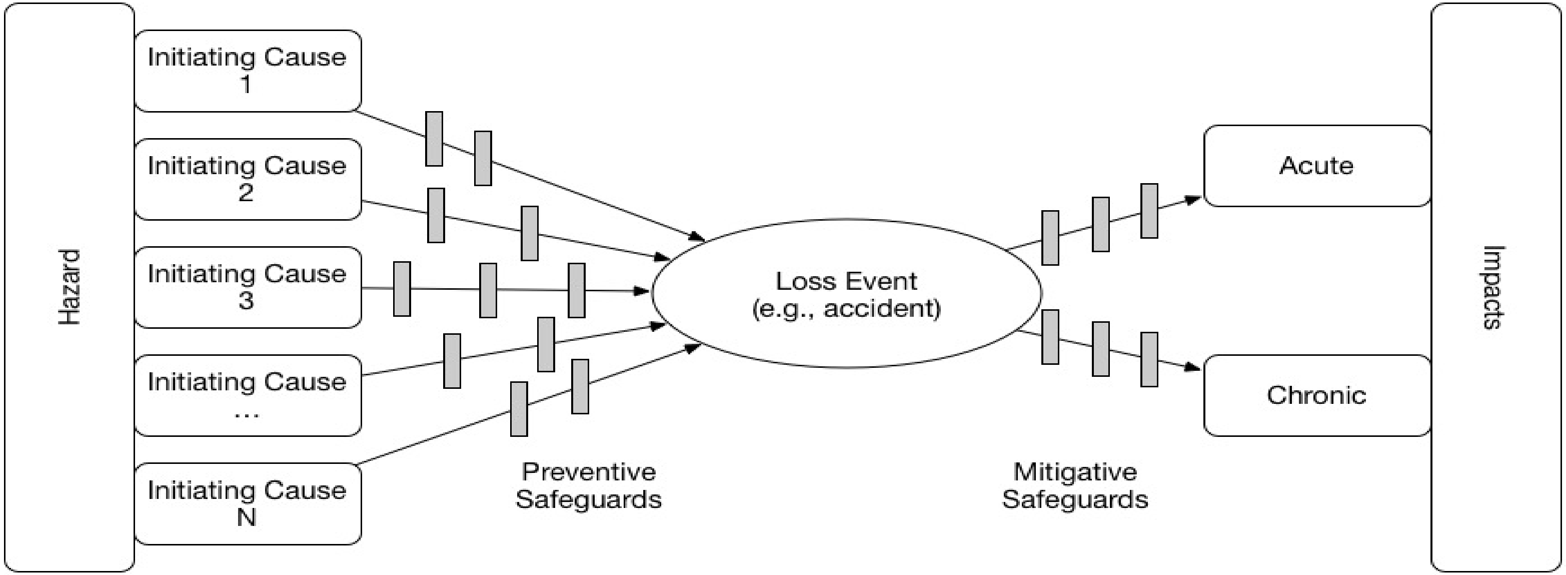
Agenda

October 17, 2018

- **Hazard Analysis (HA) Techniques**
  - What If?
  - Failure Mode Effect Analysis (FMEA)
  - Preliminary Hazard Analysis (PHA)
  - Hazard & Operability Study (HAZOP)
  - Fault Tree/ Event Tree
- **Example HA Process**
  - Preliminary Steps
  - Info. Gathered from Operations
  - What Questions Should be Asked?
  - Organizing Our Findings

Hazard Analysis Techniques

“Bow-Tie” Diagram – Hazard Analysis Process



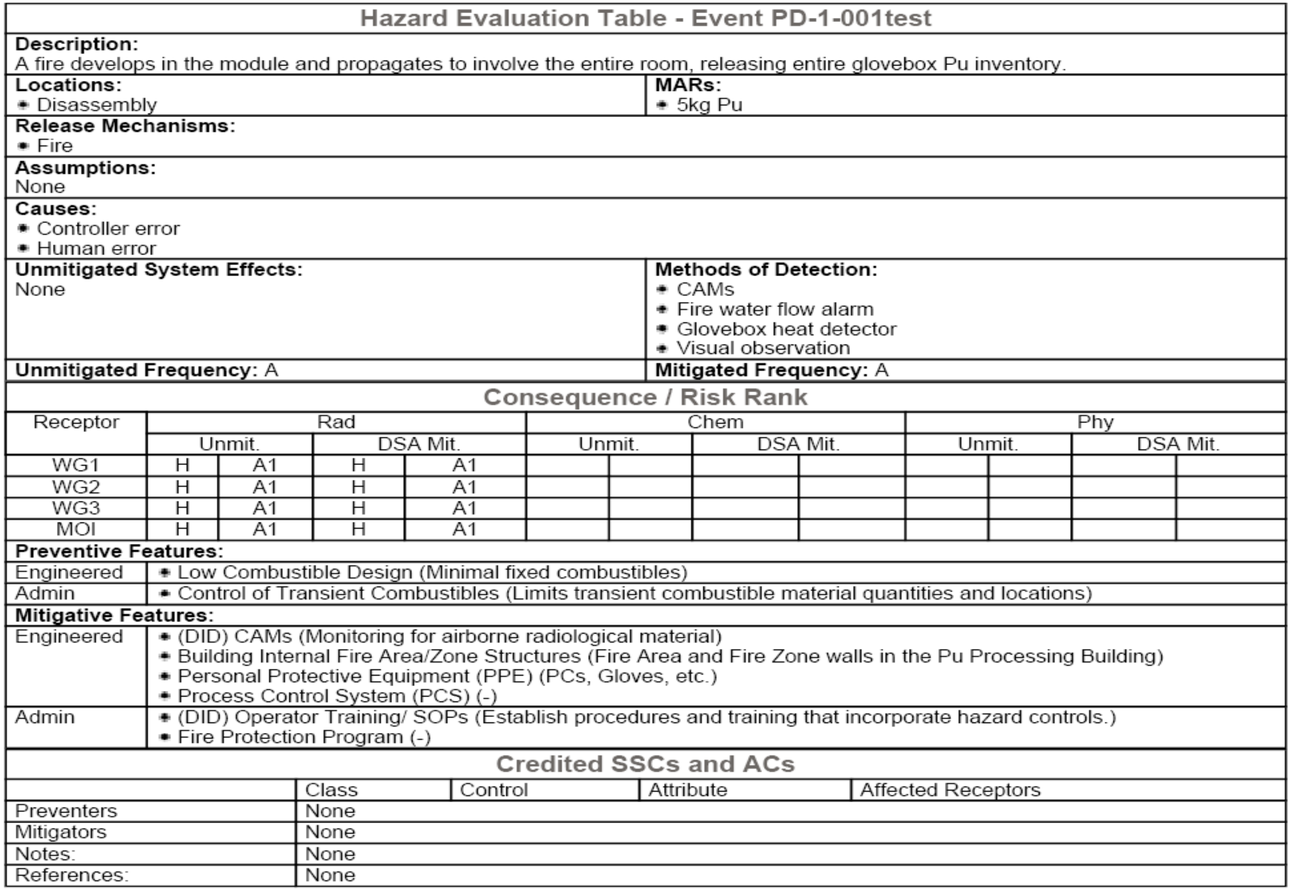
ELO 3: Hazard Analysis Techniques

***Guidelines for Hazard Evaluation Procedures* is a very useful resource to select an appropriate hazard analysis technique**

- What-If: dependent on expertise of individuals; very flexible
- HAZOP: guidewords selected for various design phases
- Fault-Tree/Event-Tree: helps define dominant accident sequences and accidents involving multiple failures (last resort)
- Failure Modes and Effects Analysis (FMEA): best for mechanical systems
- Preliminary Hazard Analysis: initial assessment of hazards

Unclassified

Example Hazard Evaluation Form



Hazard Evaluation Table - Event PD-1-001test

Description:
A fire develops in the module and propagates to involve the entire room, releasing entire glovebox Pu inventory.

Locations: • Disassembly	**MARs:** • 5kg Pu

Release Mechanisms:
- Fire

Assumptions:
None

Causes:
- Controller error
- Human error

Unmitigated System Effects: None	**Methods of Detection:** • CAMs • Fire water flow alarm • Glovebox heat detector • Visual observation
Unmitigated Frequency: A	**Mitigated Frequency:** A

Consequence / Risk Rank

Receptor	Rad				Chem				Phy			
	Unmit.		DSA Mit.		Unmit.		DSA Mit.		Unmit.		DSA Mit.	
WG1	H	A1	H	A1								
WG2	H	A1	H	A1								
WG3	H	A1	H	A1								
MOI	H	A1	H	A1								

Preventive Features:

Engineered	• Low Combustible Design (Minimal fixed combustibles)
Admin	• Control of Transient Combustibles (Limits transient combustible material quantities and locations)

Mitigative Features:

Engineered	• (DID) CAMs (Monitoring for airborne radiological material) • Building Internal Fire Area/Zone Structures (Fire Area and Fire Zone walls in the Pu Processing Building) • Personal Protective Equipment (PPE) (PCs, Gloves, etc.) • Process Control System (PCS) (-)
Admin	• (DID) Operator Training/ SOPs (Establish procedures and training that incorporate hazard controls.) • Fire Protection Program (-)

Credited SSCs and ACs

	Class	Control	Attribute	Affected Receptors
Preventers	None			
Mitigators	None			
Notes:	None			
References:	None			

What-If: Description

- Group familiar with process asks questions about hazards.
- Not highly structured like HAZOP analysis or FMEA.
- Questions begin with “What-If.”
- May address any normal, abnormal, or accident conditions.

What-If: Purpose

- **Can examine deviation from the design, construction, modification, or operating intent.**
- **Simple technique:**
  - Can be performed more quickly than most other hazard evaluation techniques.
  - But can lead to endless list of permutations
- **Produces list of questions, associated outcomes, safeguards**

FMEA: Description

- FMEA tabulates failure modes of equipment and their effects on a system or a plant.
- Failure mode describes how the equipment fails (open, closed, on, off, leaks, ruptures, sticks, etc.).

FMEA: Purpose

- Identifies single failure modes and the effect of failure on the system or plant.
- Provides recommendations for increasing equipment reliability, thus improving process safety.
- Produces table identifying each piece of equipment, failure modes/effects, estimate of worst-case consequences, and recommended changes.

PHA: Description

- **Preliminary Hazard Analysis (PHA) derived from U.S. Military Standard, *System Safety Program Requirements* [MIL-STD-882B].**
- **PHA formulates list of hazards and hazard scenarios by considering:**
  - Hazardous materials and energy sources
  - Facility layout and plant equipment;
  - Operating activities, including testing, maintenance, etc.; and
  - Safety-related interfaces among elements of the system.

PHA: Purpose

- Each hazard scenario is qualitatively evaluated to develop a relative risk ranking.
- Controls to prevent or mitigate each hazard scenario are proposed and are prioritized based on ranking.
- Often a precursor to further (more detailed) hazard and accident analysis

HAZOP: Description

- **HAZOP leader systematically guides interdisciplinary team through the plant design using:**
  - Guide words: no, less, more, part of, as well as, reverse, other than.
  - Process parameters: flow, time, frequency, mixing, pressure, etc.
  - Study nodes: points throughout the process.
    - Examples: No + Flow = No Flow;   Less + Flow = Less Flow.
    - Careful review of a process or operation in a systematic fashion to determine whether process deviations can lead to undesirable consequences

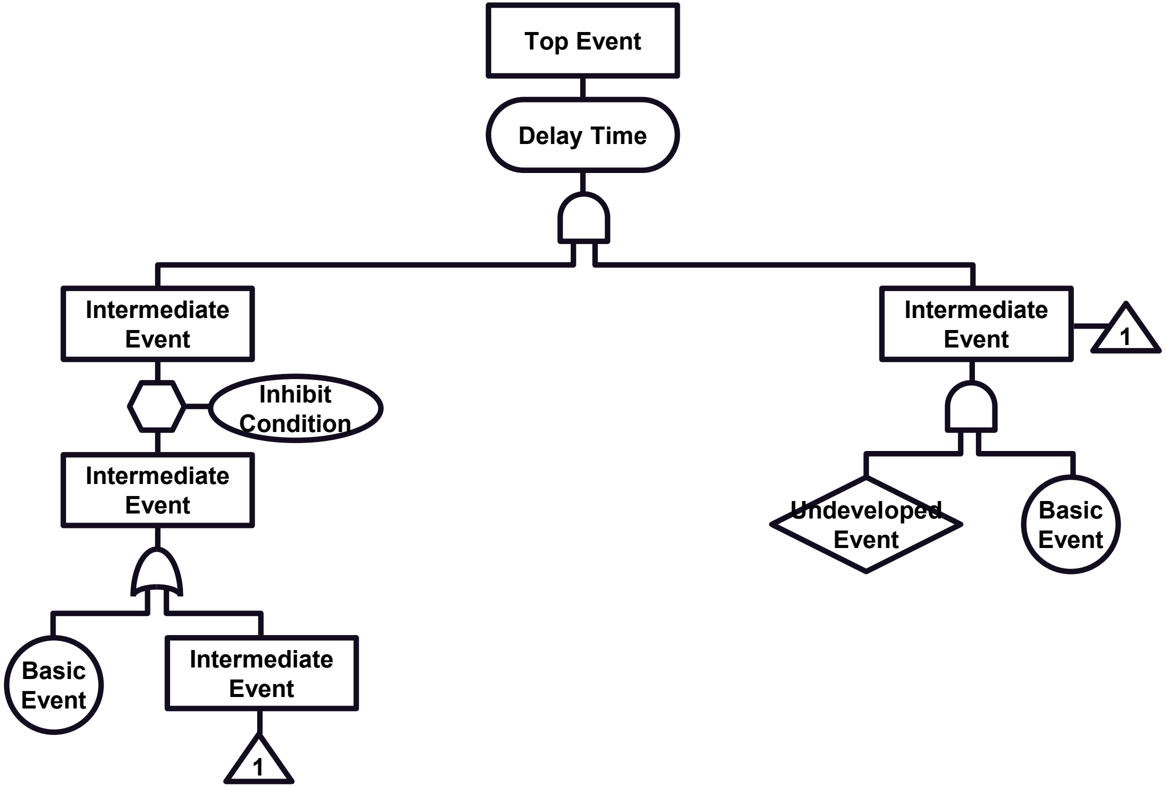
HAZOP: Purpose

- Uses a prescribed protocol to methodically evaluate the significance of deviations from the normal design intention.
- Based on the principle that several experts with different backgrounds can identify more problems when working together This same principle is beneficial to other HE techniques as well, but it is at the core of HAZOP.

Fault Tree Analysis: Description

- Focuses on a particular accident or main system failure (top event) and provides a method for determining its causes.
- Is a graphical model that displays various combinations of failures that can result in the main system failure of interest.
- As *qualitative* tool: allows the hazard analyst to focus preventive controls on the significant basic causes to reduce the likelihood of an accident.
- As *quantitative* tool: can be used as a part of probabilistic risk analysis (with probabilities assigned to events) to determine frequency bins.

Fault Tree Analysis: Example



Fault Tree Analysis: Purpose

- Often used when another HE technique has pinpointed an important accident of interest that requires more detailed analysis to determine causes and preventive controls.
- Well suited to complex, highly redundant systems, and systems vulnerable to multiple failures.

Example Hazard Analysis Process

Preliminary Steps

- **Operations requests an evaluation from NCS**
- **Obtain a description of the operation and proposed control scheme from operations personnel**
  - Determine if this provides adequate information to perform HA
- **Form HA team (Operations, Engineering, NCS, ect.)**
- **Ensure participants are aware of method to be utilized**
- **Schedule meeting with HA team**

Schedule meeting only once all parties are prepared.

Information Gathered from Operations

- Operations wants to activate a fissile material operation (FMO) in a solution processing glovebox (GB) line utilizing special nuclear material (SNM)
- The GB line includes several tanks and equipment used for processing material
- SNM will be introduced as an oxidized, solid form and dissolved/diluted to the desired concentration and purified
- Material will be introduced through an airlock from an adjacent Drop-box
- GB line is equipped with non-fissile solution lines essential to the process
- Fire suppression systems are present in the room

You probably will not get everything needed from operations up-front

What Questions Should be Asked?

- **Operations wants to activate a fissile material operation (FMO) in a solution processing glovebox (GB) line utilizing special nuclear material (SNM)**
  - How much material do you NEED to process? (Hint: Ops probably WANTS more)
  - What material forms are allowed?
  - What is the single parameter sub-critical mass of the SNM dry?
  - What is the single parameter sub-critical mass of the SNM in solution?
  - Is over-mass credible? Double batch?

Parameters effected: Mass/Form, Moderation

What Questions Should be Asked? (Cont’d)

- **Info from ops: “SNM will be introduced in an oxidized, solid form and dissolved/diluted to the desired concentration and purified”**
  - Can additional forms be present in an upset condition?
  - What is the purity of the SNM?
  - Can we credit a lower enrichment?
  - Can we credit any absorbers inherent in the process? (hint: usually not)

Parameters effected: Mass/Form, Enrichment/Assay, Absorption

What Questions Should be Asked? (Cont'd)

- **Info from ops: "The GB line includes several tanks and equipment used for processing material"**
  - Are these geometrically safe tanks?
  - Can we credit spacing between tanks?
  - What is the potential for a buildup of SNM inside the tank?
  - What kind of equipment/supplies will be used inside the box or nearby?
  - Are there any accumulation locations inside the GB line?
  - How do we deal with contaminated waste generated?

Parameters effected: Geometry, Volume, Reflection

What Questions Should be Asked? (Cont’d)

- **Info from ops: “Material will be introduced through an airlock from an adjacent Drop-box”**
  - Does this previously evaluated DB FMO allow for your material?
  - Is staging allowed in the FMO?
  - Are there any adjacent FMOs/Storage Locations present within 12 in?
  - Are mobile FMOs allowed in the room?
  - What form and route will SNM exit the FMO?

Parameters effected: Mass/Form, Interaction

What Questions Should be Asked? (Cont'd)

- **Info from ops: "GB is equipped with non-fissile solution lines essential to the process"**
  - Could these solution lines introduce additional moderator/reflector?
  - Are crit. drains present in the boxes?

Parameters effected: Moderation, Reflection

What Questions Should be Asked? (Cont’d)

- **Info from ops: “Fire suppression systems are present in the room”**
  - In case of fire, do we need to consider water ingress from sprinkler activation?
  - What are pathways in which sprinkler water could enter a GB?
  - Is inadvertent activation credible?
  - Is fire inside the GB credible? Inert atmosphere GB?

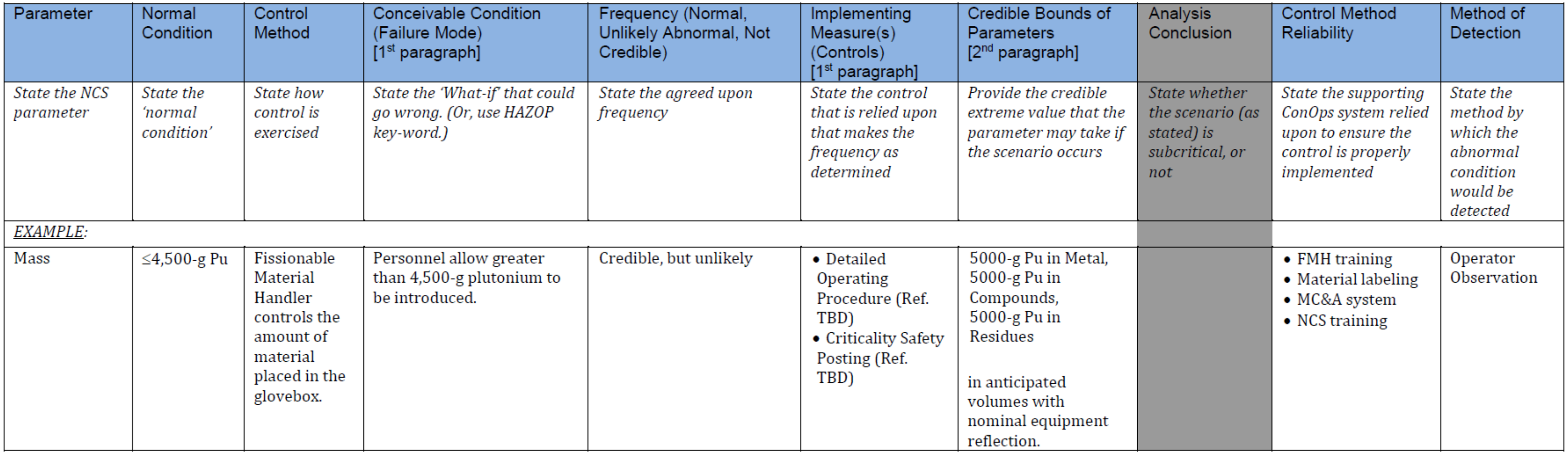
Parameters effected: Moderation, Reflection

What Questions Should be Asked? (Cont'd)

- **Consider the concurrent loss of multiple parameters**
- **Design basis (DB) event:**
  - Is GB seismically qualified?
  - Can GB fall into a more reactive configuration or co-locate with another FMO?
  - Is it credible for a DB event to cause sprinkler activation?

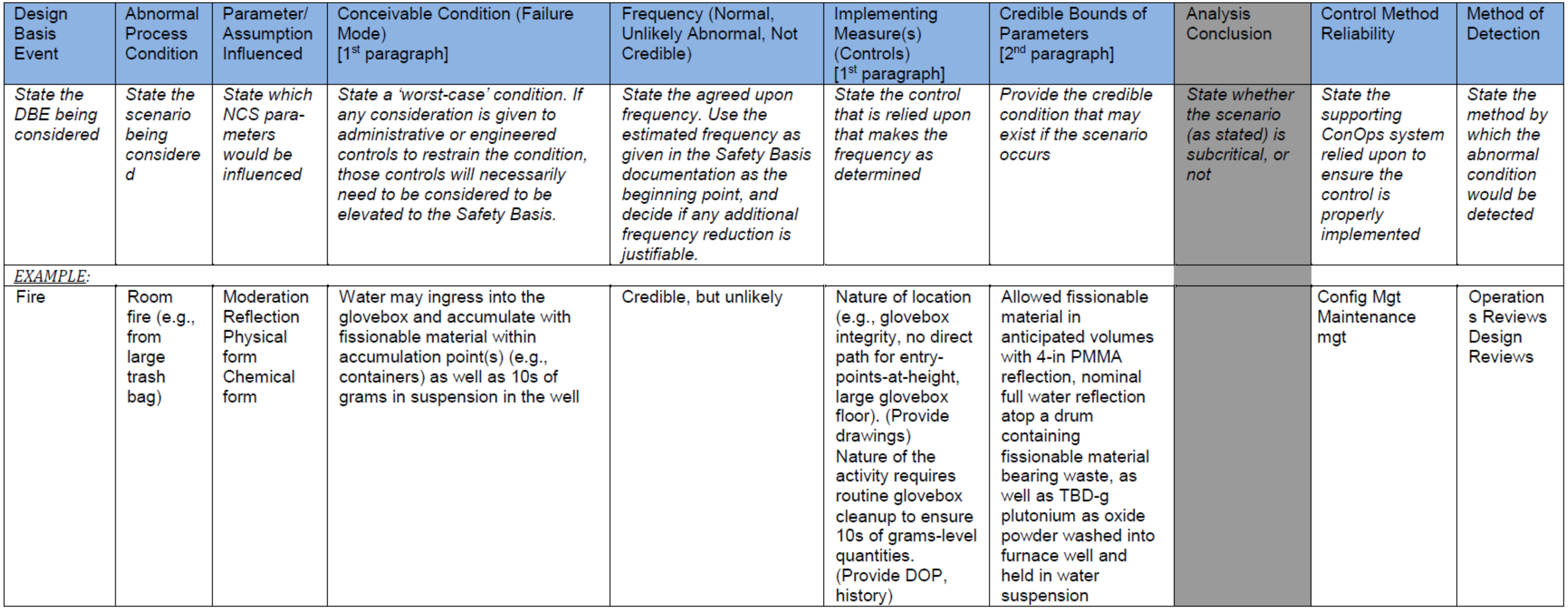
Parameters effected: Multiple parameters based on credible accident

How do We Organize Our Findings?



Parameter	Normal Condition	Control Method	Conceivable Condition (Failure Mode) [1st paragraph]	Frequency (Normal, Unlikely Abnormal, Not Credible)	Implementing Measure(s) (Controls) [1st paragraph]	Credible Bounds of Parameters [2nd paragraph]	Analysis Conclusion	Control Method Reliability	Method of Detection
State the NCS parameter	*State the 'normal condition'*	*State how control is exercised*	*State the 'What-if' that could go wrong. (Or, use HAZOP key-word.)*	*State the agreed upon frequency*	*State the control that is relied upon that makes the frequency as determined*	*Provide the credible extreme value that the parameter may take if the scenario occurs*	*State whether the scenario (as stated) is subcritical, or not*	*State the supporting ConOps system relied upon to ensure the control is properly implemented*	*State the method by which the abnormal condition would be detected*
<u>EXAMPLE</u>:									
Mass	≤4,500-g Pu	Fissionable Material Handler controls the amount of material placed in the glovebox.	Personnel allow greater than 4,500-g plutonium to be introduced.	Credible, but unlikely	• Detailed Operating Procedure (Ref. TBD) • Criticality Safety Posting (Ref. TBD)	5000-g Pu in Metal, 5000-g Pu in Compounds, 5000-g Pu in Residues in anticipated volumes with nominal equipment reflection.		• FMH training • Material labeling • MC&A system • NCS training	Operator Observation

How do We Organize Our Findings? (DB Event)



Design Basis Event	Abnormal Process Condition	Parameter/ Assumption Influenced	Conceivable Condition (Failure Mode) [1st paragraph]	Frequency (Normal, Unlikely Abnormal, Not Credible)	Implementing Measure(s) (Controls) [1st paragraph]	Credible Bounds of Parameters [2nd paragraph]	Analysis Conclusion	Control Method Reliability	Method of Detection
State the DBE being considered	*State the scenario being considered*	*State which NCS parameters would be influenced*	*State a 'worst-case' condition. If any consideration is given to administrative or engineered controls to restrain the condition, those controls will necessarily need to be considered to be elevated to the Safety Basis.*	*State the agreed upon frequency. Use the estimated frequency as given in the Safety Basis documentation as the beginning point, and decide if any additional frequency reduction is justifiable.*	*State the control that is relied upon that makes the frequency as determined*	*Provide the credible condition that may exist if the scenario occurs*	*State whether the scenario (as stated) is subcritical, or not*	*State the supporting ConOps system relied upon to ensure the control is properly implemented*	*State the method by which the abnormal condition would be detected*
<u>EXAMPLE</u>:									
Fire	Room fire (e.g., from large trash bag)	Moderation Reflection Physical form Chemical form	Water may ingress into the glovebox and accumulate with fissionable material within accumulation point(s) (e.g., containers) as well as 10s of grams in suspension in the well	Credible, but unlikely	Nature of location (e.g., glovebox integrity, no direct path for entry-points-at-height, large glovebox floor). (Provide drawings) Nature of the activity requires routine glovebox cleanup to ensure 10s of grams-level quantities. (Provide DOP, history)	Allowed fissionable material in anticipated volumes with 4-in PMMA reflection, nominal full water reflection atop a drum containing fissionable material bearing waste, as well as TBD-g plutonium as oxide powder washed into furnace well and held in water suspension		Config Mgt Maintenance mgt	Operations Reviews Design Reviews